IN THE CLAIMS:

Please amend the claims such that the pending claims read as follows:

1. (Amended) A method for operating a filer including the steps of:

receiving at a first location a request from a user for an object;

processing said request at a second location, wherein said step of processing includes at least one of the following: (1) searching for one or more recognizable patterns of data within said object, (2) compressing said object, and (3) encrypting said object;

responding to said request, wherein said step of responding includes delivery of a response to said user.

a4

2. The method of claim 1, wherein said request is in an electronic form.

3. The method of claim 1, wherein said object is a file.

4. (Amended) The method of claim 3, wherein said step of processing said request further includes the steps of:

creating an access path from said filer to a processing cluster;

processing said file in said processing cluster; and

generating a scan report wherein, said scan report is responsive to said processing of said file in said processing cluster.

5. The method of claim 4, wherein said step of creating an access path includes sending the ID and path of said file from said filer to said processing cluster.

6. The method of claim 5, wherein said step of sending is accomplished using non-uniform memory access.

a4

7. The method of claim 5, wherein said step of sending is accomplished using a communications network.

8. The method of claim 5, wherein said step of sending is accomplished using a direct connection.

9. The method of claim 4, wherein said step of processing of said file is performed by said processing cluster in a round robin fashion for subsequent files received.

10. The method of claim 4, wherein said step of processing of said file is accomplished in parts by more than one device in said processing cluster.

11. The method of claim 4, wherein all files stored on said filer are scanned in a logical continuous manner.

12. The method of claim 4, wherein said scan report contains a set of status data relating to said processing of said file.

13. The method of claim 12, wherein said status data includes at least one data element identifying the presence or non-presence of a virus in said file.

a4

14. The method of claim 13, wherein said report is transferred to said filer.

15. The method of claim 14, wherein said report is stored in a first database.

16. The method of claim 15, wherein the necessity for subsequent scanning of said file is a function of determining whether said database contains said report relating to said file and whether said file has changed since last accessed.

17. The method of claim 16, wherein the necessity for subsequent scanning of said file is a function of determining whether additional virus identification data files have been added to said processing cluster.

18. The method of claim 1, wherein said delivery of a response is said file.

19. The method of claim 1, wherein said delivery of a response includes notification to said user that said file is unavailable.

20. The method of claim 1, wherein said step of responding to said request includes sending said user a copy of said scan report.

a4

21. (Amended) An apparatus for operating a filer including:

means for receiving at a first location a request from a user for an object;

means for processing said request at a second location, wherein said means for processing includes at least one of the following: (1) means for searching for one or more recognizable patterns of data within said object, (2) means for compressing said object, and (3) means for encrypting said object:

means for responding to said request, wherein said means for responding includes delivery of a response to said user.

22. The apparatus of claim 21, wherein said object is a file.

23. (Amended) The apparatus of claim 22, wherein said means for processing said request further includes:

means for creating an access path from said filer to a processing cluster;

means for processing said file in said processing cluster; and

means for generating a scan report wherein, said scan report is responsive to said processing of said file in said processing cluster.

24. The apparatus of claim 23, wherein said means for creating an access path includes means for sending the ID and path of said file from said filer to said processing cluster.

a4

25. (Amended) The apparatus of claim 24, wherein said sending is accomplished using non-uniform memory access.

26. (Amended) The apparatus of claim 24, wherein said sending is accomplished using a communications network.

27. (Amended) The apparatus of claim 24, wherein said sending is accomplished using a direct connection.

28. (Amended) The apparatus of claim 23, wherein said processing of said file is performed by said processing cluster in a round robin fashion for subsequent files received.

29. (Amended) The apparatus of claim 23, wherein said processing of said file is performed on atomic units of said file by more than one device in said processing cluster.

30. The apparatus of claim 23, wherein all files stored on said filer are scanned in a logical continuous manner.

31. The apparatus of claim 23, wherein said scan report contains a set of status data relating to said processing of said file.

a4

32. The apparatus of claim 31, wherein said status data includes at least one data element identifying the presence or non-presence of a virus in said file.

33. The apparatus of claim 31, wherein said report is transferred to said filer.

34. The apparatus of claim 33, wherein said report is stored in a first database.

35. The apparatus of claim 34, wherein the necessity for subsequent scanning of said file is a function of determining whether said database contains said report relating to said file and whether said file has changed since last accessed.

36. The apparatus of claim 35, wherein the necessity for subsequent scanning of said file is a function of determining whether additional virus identification data files have been added to said processing cluster.

37. The apparatus of claim 21, wherein said delivery of a response is delivery of said file.

38. The apparatus of claim 21, wherein said delivery of a response includes delivery of notification to said user that said file is unavailable.

a4

39. (Amended) The apparatus of claim 21, wherein said responding to said request includes sending said user some portion of said scan report.

40. (New) A method of attempting to provide virus protection in a client-server environment, comprising the steps of:

receiving a request at a server for a file;

sending an identifier for the file to a scanning device that scans the file for viruses;

receiving an indication from the scanning device as to whether or not the file is safe to send from the server; and

responding to the request by sending the file if the indication is that the file is safe to send.

41. (New) A method as in claim 40, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

42. (New) A method as in claim 40, wherein the request is received from and the file is sent to a client device.

43. (New) A method as in claim 40, wherein the server is a web server.

a4

44. (New) A method as in claim 40, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

45. (New) A method as in claim 44, wherein the cluster of devices is a cluster of interconnected personal computers.

46. (New) A method of attempting to provide virus protection in a client-server environment, comprising the steps of:

maintaining a database that indicates if files served by a server are safe to send from the server;

receiving a request at the server for a file;

if the database indicates that the file is safe to send, responding to the request by sending the file; and

if the database does not indicate that the file is safe to send, then sending an identifier for the file to a scanning device that scans the file for viruses, receiving an indication from the scanning device as to whether or not the file is safe to send from the server, and responding to the request by sending the file if the indication is that the file is safe to send.

47. (New) A method as in claim 46, wherein maintaining the database further comprises the steps of:

a4

tracking received indications from the scanning device; and

tracking accesses to the file.

48. (New) A method as in claim 47, wherein a tracked indication in the database that the file is safe to send is cancelled if the file has changed since the tracked indication was incorporated into the database.

49. (New) A method as in claim 46, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

50. (New) A method as in claim 46, wherein the request is received from and the file is sent to a client device.

51. (New) A method as in claim 46, wherein the server is a web server.

52. (New) A method of attempting to provide virus protection in a client-server environment, comprising the steps of:

receiving from a server, at a scanning device connected to the server, an identifier for a file stored on mass storage for the server;

scanning the file for viruses; and

reporting an indication to the server as to whether or not the file is infected.

53. (New) A method as in claim 52, further comprising the step of changing, deleting, or otherwise modifying the file based on a result of scanning the file for viruses.

54. (New) A method as in claim 52, wherein the server is a web server.

55. (New) A method as in claim 52, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

56. (New) A method as in claim 55, wherein the cluster of devices is a cluster of interconnected personal computers.

57. (New) A server that attempts to provide virus protection in a client-server environment, comprising:

a communication link to client devices;

mass storage for files; and

a processor that executes instructions in order to send requested files to the client devices, the instructions also including instructions (a) to receive a request for a file, (b) to send an identifier for the file to a scanning device that scans the file for viruses, (c) to receive an indication from the scanning device as to whether or not the file is safe to send from the server, and (d) to respond to the request by sending the file if the indication is that the file is safe to send.

58. (New) A server as in claim 57, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

59. (New) A server as in claim 57, wherein the request is received from and the file is sent to a client device.

60. (New) A server as in claim 57, wherein the server is a web server.

61. (New) A server as in claim 57, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

62. (New) A server as in claim 61, wherein the cluster of devices is a cluster of interconnected personal computers.

63. (New) A server that attempts to provide virus protection in a client-server environment, comprising:

a communication link to client devices;

mass storage for files; and

a processor that executes instructions in order to send requested files to the client devices, the instructions also including instructions (a) to maintain a database that indicates if files served by a server are safe to send from the server, (b) to receive a request at the server for a file, (c) if the database indicates that the file is safe to send, to respond to the request by sending the file, and (d) if the database does not indicate that the file is safe to send, then to send an identifier for the file to a scanning device that scans the file for viruses, to receive an indication from the scanning device as to whether or not the file is safe to send from the server, and to respond to the request by sending the file if the indication is that the file is safe to send.

64. (New) A server as in claim 63, wherein the instructions to maintain the database further comprise instructions to track received indications from the scanning device, and to track accesses to the file.

65. (New) A server as in claim 64, wherein a tracked indication in the database that the file is safe to send is cancelled if the file has changed since the tracked indication was incorporated into the database.

66. (New) A server as in claim 63, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

a4

67. (New) A server as in claim 63, wherein the request is received from and the file is sent to a client device.

68. (New) A server as in claim 63, wherein the server is a web server.

69. (New) A scanning device that attempts to provide virus protection for a server in a client-server environment, comprising:

a communication link to the server; and

a processor that executes instructions, the instructions including instructions (a) to receive from the server an identifier for a file stored on mass storage for the server, (b) to scan

the file for viruses, and (c) to report an indication to the server as to whether or not the file is infected.

70. (New) A scanning device as in claim 69, wherein the instructions further comprise instructions to change, delete, or otherwise modify the file based on a result of scanning the file for viruses.

71. (New) A scanning device as in claim 69, wherein the server is a web server.

Q4

72. (New) A scanning device as in claim 69, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

73. (New) A scanning device as in claim 72, wherein the cluster of devices is a cluster of interconnected personal computers.

74. (New) Storage containing information including instructions, the instructions executable by a processor to attempt to provide virus protection in a client-server environment, the instructions comprising the steps of:

receiving a request at a server for a file;

sending an identifier for the file to a scanning device that scans the file for viruses;

receiving an indication from the scanning device as to whether or not the file is safe to send from the server; and

responding to the request by sending the file if the indication is that the file is safe to send.

75. (New) Storage as in claim 74, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

a4

76. (New) Storage as in claim 74, wherein the request is received from and the file is sent to a client device.

77. (New) Storage as in claim 74, wherein the server is a web server.

78. (New) Storage as in claim 74, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

79. (New) Storage as in claim 78, wherein the cluster of devices is a cluster of interconnected personal computers.

80. (New) Storage containing information including instructions, the instructions executable by a processor to attempt to provide virus protection in a client-server environment, the instructions comprising the steps of:

maintaining a database that indicates if files served by a server are safe to send from the server;

receiving a request at the server for a file;

if the database indicates that the file is safe to send, responding to the request by sending the file; and

if the database does not indicate that the file is safe to send, then sending an identifier for the file to a scanning device that scans the file for viruses, receiving an indication from the scanning device as to whether or not the file is safe to send from the server, and responding to the request by sending the file if the indication is that the file is safe to send.

81. (New) Storage as in claim 80, wherein maintaining the database further comprises the steps of:

tracking received indications from the scanning device; and

tracking accesses to the file.

82. (New) Storage as in claim 81, wherein a tracked indication in the database that the file is safe to send is cancelled if the file has changed since the tracked indication was incorporated into the database.

83. (New) Storage as in claim 80, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

84. (New) Storage as in claim 80, wherein the request is received from and the file is sent to a client device.

85. (New) Storage as in claim 80, wherein the server is a web server.

a4

86. (New) Storage containing information including instructions, the instructions executable by a processor to attempt to provide virus protection in a client-server environment, the instructions comprising the steps of:

receiving from a server, at a scanning device connected to the server, an identifier for a file stored on mass storage for the server;

scanning the file for viruses; and

reporting an indication to the server as to whether or not the file is infected.

87. (New) Storage as in claim 86, wherein the instructions further comprise the step of changing, deleting, or otherwise modifying the file based on a result of scanning the file for viruses.

88. (New) Storage as in claim 86, wherein the server is a web server.

89. (New) Storage as in claim 86, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

90. (New) Storage as in claim 89, wherein the cluster of devices is a cluster of interconnected personal computers.

91. (New) Storage containing information including instructions, the instructions executable by a processor to operate a filer, the instructions comprising the steps of:

a4

receiving at a first location a request from a user for an object;

processing said request at a second location, wherein said step of processing includes at least one of the following: (1) searching for one or more recognizable patterns of data within said object, (2) compressing said object, and (3) encrypting said object;

responding to said request, wherein said step of responding includes delivery of a response to said user.